05-PR-M-0002 Issuance date: **13 OCT 2005**

INFORMATION ASSURANCE (IA) TRAINING:
VERSION 1.0

1. Overview

The IA workforce focuses on the operation and management of Information Assurance (IA) capabilities for Department of Defense (DoD) systems and networks. IA ensures that adequate security measures and established IA policies and procedures are applied to all Information Systems (IS) and networks. The IA workforce includes all privileged users and IA managers who perform any of the responsibilities or functions described in draft DoD 8570.1M chapters 3 - 5. These responsibilities include: developing, testing, deploying, operating, administering, troubleshooting, managing, and retiring Department of Defense (DoD) information systems. To support the warfighter in a highly effective and professional manner, the Army must ensure that appropriate levels of IA awareness, training, education certification and workforce management are provided to the IA workforce and Information System users that commensurate with their respective responsibilities.

The Information Assurance (IA) training audience includes military, civilian, foreign nationals and contractor personnel. In addition to being able to demonstrate the required level of technical and/or managerial skills and experience, it is DoD policy (DoDD 8570.1, 15 Aug 04) that "the IA workforce knowledge and skills be verified through standard certification testing." Consequently, Army IA personnel must attain and maintain Information Technology (IT)/IA certifications appropriate for the technical and/or managerial requirements of their position. In some cases, this will include passing one or more certification exams. IA Workforce personnel in Technical and Management Level positions must complete eighty hours of sustainment training biannually or as required to maintain certification status, whichever is greater.

This Best Business Practice (BBP) describes other regulatory requirements established by the draft DoD 8570.1M as well as procedures for tracking the training and certification completing statistics. The IA workforce, technical and management levels described in draft DoD 8570.1-M are listed in this BBP. Programs such as, network compliance scanning and vulnerability assessments will also have training addressed in their respective BBPs. Updates to this BBP will be provided when the draft 8570.1M is signed by DoD.

2. IA BBP Subject Matter Expert (SME) or Point(s) of Contact (POC):

NETCOM IA Directorate; NETC- EST-A

Name:	Phyllis Bailey	(703) 602-7408
	Doris Wright	(703) 602-7420

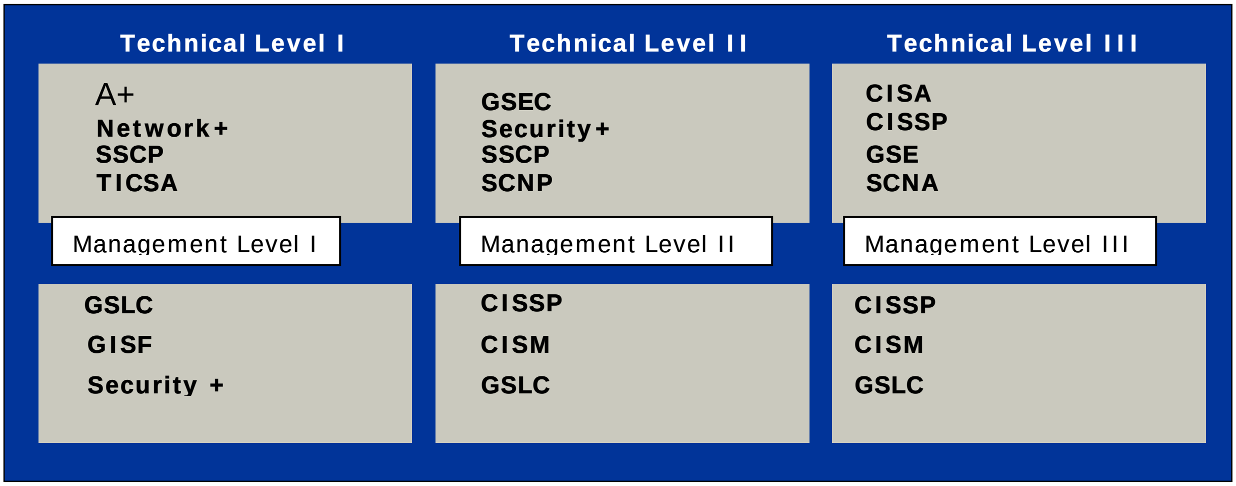
3. Description of Former State: Army and DoD regulations do not require specific certification and training at different levels. This BBP will lay out the training and certification requirements for Technical and Management levels.

4. Description of Changes Instituted: The IA Workforce must become familiar with the training and certification requirements in accordance with their title and position. Personnel who have privileged access and limited privileged access (IT-1 and IT-II) are required to be IA trained, certified and maintain their certifications. All managers need to be fully aware that foreign nationals can not be IT-1 without consent of the Local DAA, the data owner and approval by HQDA CIO/G6.

5. Description of End State: An IA trained and certified workforce with enhanced capabilities to combat threats against Army information, networks and information systems.

6. Description of Required Resources: Army is currently working with DoD to decrease the cost for obtaining a commercial certification. Military personnel can use the GI Bill to cut the cost for the COMPTIA Security+, A+, Network+, among others. They must contact their education center for more information. Civilians are authorized to pay for certification training through their appropriate organization's funds per Manpower and Reserve Affairs memorandum dated 20 June 2003. The IA workforce may incur some cost for obtaining the required certifications that are listed in Table 1. Some certification courses are available online at no-cost to the activity; however certification testing cannot be taken online. The cost of individual certification tests range from $100 to $500. There are also TDY, tuition, and travel costs for specific technical training.

Table 1.



Technical Level I	Technical Level II	Technical Level III
A+ Network+ SSCP TICSA	GSEC Security+ SSCP SCNP	CISA CISSP GSE SCNA
Management Level I	Management Level II	Management Level III
GSLC GISF Security +	CISSP CISM GSLC	CISSP CISM GSLC

7. Description of Derived Benefits Resulting from Implementation: A more secure use of Army information, networks and information systems in support of the warfighter and garrison activities, including the reduction of vulnerabilities that can be exploited due to systems and networks being administered by an inadequately trained and unskilled workforce.

8. Administrative Requirements:

a. The minimum IA training requirements must be completed within six months of assignment to IA duties. Certification and validated testing (with a passing score), must be completed in accordance with the individual's performance and evaluation process. This includes duties as system/network administrators, etc., as well as typical IA positions such as Information Assurance Manager (IAM), Information Assurance Security Officer (IASO), and Information Assurance Program Manager (IAPM) staff. Refresher training is required between 18 to 24 months, after initial training (AR 25-2a (8) (a)).

b. The E-Learning modules (SkillPort) for IA training are available at http://usarmy.SkillPort.com via the AKO portal at https://www.us.army.mil. Contractors who require access to SkillPort for IA training will coordinate their request through their IAM or IAPM with the NETCOM IA Division Point of Contacts (POC) doris.wright@us.army.mil and Phyllis.bailey@us.army.mil.

.

c. The IA workforce will provide initial information and status updates as they complete training/certification courses in the Asset and Vulnerability Tracking Resource (A&VTR) Database. New IA workforce personnel will register in A&VTR at time of appointment. DoD policy requires status of all positions with IA responsibilities, regardless of occupational specialty, or whether the duty is performed full-time or part-time as an additional/embedded duty. Each of these positions will be aligned to an IA category and level, and documented in the appropriate database.

.

d. IA workforce personnel are encouraged to pursue educational opportunities through the IA Scholarship program (IASP) to obtain advanced degrees with IA concentrations.

9. Related BBPs: None

10. Products:

- E-learning (SkillPort) is available at https://usarmy.skillport.com
- DISA web-based training available at http://www.iase.disa.mil
- MACOM-approved IT/IA training and vendor specific training uniquely focused on passing certification tests.
- IASP program is: http://www.defenselink.mil/nii/iasp/.
- Manpower and Reserve Affairs Memorandum, Subject: Payment of Expenses to Obtain Professional Credentials for Army Civilian Employees: http:/cpol.army.mil/library/train/tld-062003.html.

11. Description: Refer to table 1, IA Workforce Certification (abstract from draft 8570.1M) for IT and IM training certifications**.** The certification/training requirements for the IA roles and the IA workforce are listed under the titles, as follows:

a. **Management Level I: Information Assurance Security Officer (IASO) and Information Management Officers (IMO)/Information Systems Officers (ISO):** The minimum training requirements must be completed within 6 months of assuming the above positions. These positions refer to individuals who have 0-5 years of management experience and must be knowledgeable in their organization's Computing Environment. The IASO/IMO/ISO will be designated as Information Technology I (IT-I/II/or III).

Minimum Training Requirements

(1). IASO course online (https://ia.gordon.army.mil/iaso) – approximately 1 hour (on-line from any computer-home or office).

(2). E-learning Security + modules (SkillPort, CIO G6/NETCOM IA Phase I>SYO-101 Security+ (7 modules)) – approximately 3-4 working days or a certification listed in Management I Level. Training can be taken on-line via the internet on an office or home computer. The E-learning Security + module builds on the certification for Security +.

Certification Requirements: In order to continue to build to a certified IA workforce for Manager Level I , the IASO/IMO/ISO need to continue their education and complete one of the certifications listed in table one. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process.

** The IA directorate will work towards building a virtual training solution for management level one certification testing. The high turnover rate of this position makes this approach necessary for the Army to achieve compliance with the DoD instruction and manual. When this product is available, and has been approved by DoD, it will be released for use Army-wide.

b. **Management Level II: Installation/Major Subordinate Commands (MSC)/posts, Major Command (MACOM)/ Tactical Units/PEOs Level Information Assurance Manager (IAM) and Certification Agent (CA):** The minimum training requirements must be completed within 6 months of assuming the IAM position. This position refers to individuals who have at least 5 years of management experience and must be knowledgeable in their organization's Network Environment. Management Level II personnel must be knowledgeable of IA policy, procedures and workforce structure to develop, implement and maintain a secure Network Environment. They typically reports to an IA Management Level III (Enclave) Manager or DAA or senior management for network operational requirements. The IAM position is designated as IT-I/II or III per AR 25-2. The CA is designated as IT-I per AR 25-2.

Minimum Training Requirements

(1). IASO course online (https://ia.gordon.army.mil/iaso) – approximately 1 hour.

(2). E-learning - Certified Information Systems Security Professional (CISSP) modules (SkillPort, CIO G6/NETCOM IA Phase I> Certified Information Systems Security Professional (CISSP) -5 modules) - approximately 3-5 working days (on-line course from any computer- home or office).

(3). CD ROM, DoD Certifier Fundamentals from http://iase.disa.mil **(CA only complete items 1-3)** approximately 1 hour.

Certification Requirements: In order to continue to build to a certified IA workforce for Level II manager, the IAM needs to continue their education and complete one of the certifications listed in Manager Level II area. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process. The completion of certification testing is required.

c. **Management Level III: Regional Chief Information Officer Director and Information Assurance Program Manager (IAPM)//CA**: The minimum training requirements must be completed within 6 months of assuming the Director/IAPM/CA position. This position refers to individuals who have at least 10 years of management experience and must be knowledgeable in their Regional Enclave Environment. They must be knowledgeable of IA policy, procedures and workforce structure to develop, implement and maintain a secure enclave environment. Management Level III Director/IAPM/CA typically reports to a DAA for IA issues and senior managers for enclave operational requirements. These individuals need to be able to translate strategic plans and technical guidance provided by NETCOM into objectives, strategies and architectural guidance.

Minimum Training Requirements

(1). E-learning - Certified Information Systems Security Professional (CISSP) modules (SkillPort, CIO G6/NETCOM IA Phase I> Certified Information Systems Security Professional (CISSP) -5 modules) - approximately 3-5 working days (on-line course from any computer- home or office).

(2). CD ROM, DoD Certifier Fundamentals from http://iase.disa.mil **(CA only complete items 1-2)** CBT 1.5 hours.

Certification Requirements: In order to continue to build to a certified IA workforce for Level III manager, the Director/IAPM/CA need to continue their education and obtain one of the certifications in the Management Level III area. The completion of certification testing is required. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process.

d. **Management Level III: Designated Approving Authority (DAA)**: The minimum training requirements must be completed within 6 months of assuming the DAA position. The DAA must be a U.S. citizen and have a level of authority commensurate with accepting, in writing, the risk of operating Information Systems under their purview.

(1). Complete the DoD DAA computer-based training (CBT) product. The CBT title, "DAA Designated Approving Authority," is available at http://iase.disa.mil/. Keep certificate of completion on file at the organization. CBT takes approximately 2-3 hours.

(2). **The DAA must recertify every three years.**

e. **Technical Level I:** System Administrator (SA)/ Network Manager (NM)/Network Officer (NO). The minimum training requirements must be completed within 6 months of assuming the Technical Level I SA/ NM/NO position. Normally the Level I SA/NM/NO has 0-4 years of experience in IA technology or a related field and must be knowledgeable in their organization's Computing Environment (CE). They must know how to apply basic knowledge of IA concepts, practices and procedures within the CE. Level I SA/NM/NOs are usually individuals with **Limited privileged access** to the Computing Environment and works under immediate supervision and typically reports to a Computing Environment manager. They are designated as IT-II per AR 25-2.

Minimum Training Requirements (all)

(1). IASO course (https://ia.gordon.army.mil) – Approximately 1 hour.

(2). IA Technical Level 1 course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) - Approximately 5-7 days.

(3). Network Security Issues (SkillPort>CIO-G6/NETCOM Information Assurance>CIO-G6/NETCOM IA Phase I>Net Safety>Network Security Issues – 1 module (3.5 hours).

Certification Requirements: In order to continue to build to a certified IA workforce for Technical Level I , the SA/NM/NO needs to continue their education and complete one of the certifications in the Technical Level I area. The completion of certification testing is required. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process.

f. **Technical Level II:** System Administrator (SA)/ Network Manager (NM) Network Officer (NO). The minimum training requirements must be completed within 6 months of assuming the Technical Level II SA/ NM/NO position. Normally the Level II SA/NM/NO has 3-7 years of experience in IA technology or a related field and must be knowledgeable in their organization's NE and advance training in their CE. They must master the functional requirements of the IA Technical Level I position and be able to apply knowledge and experience with standard IA concepts, practices and procedures within the network environment. The Level II SA/NM/NO is usually individuals with **Privileged access** to the Computing Environment and works under general supervision and typically reports to a Level III Network Manager. They are designated as IT-I per AR 25-2.

Minimum Training Requirements

(1). IASO course (https://ia.gordon.army.mil)

(2). IA Technical Level 1 course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) - Approximately 5-7 days

(3). Technical level 2, 10 day SA/NM course. Schedule and locations located at http://ia.gordon.army.mil.

Certification Requirements: In order to continue to build to a certified IA workforce for Technical Level II , the SA/NM/NO needs to continue their education and complete one of the certifications in the Technical Level II area. The completion of certification testing is required. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process. The Level II supervisor will notify the IA professional if she/he needs to attend the Level III certification courses held at the NGB or the U.S. Army Reserve (USAR) training facilities. The Security + module in SkillPort build on the Security + certification.

g. **Technical Level III: Regional Chief Information Officer System Administrator (SA)/ Network Manager (NM) Network Officer (NO)**. The minimum training requirements must be completed within 6 months of assuming the Technical Level III SA/ NM/NO position. Normally the Level III SA/NM/NO has 7 years of experience in IA technology or a related field and must be knowledgeable in their organization's NE and advance training in their CE. They must be an expert in all functional requirements of both IA Technical Level I and IA Technical Level II positions. They must be able to apply extensive knowledge of a variety of IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems. They work independently to quickly and completely solve problems and may lead and direct the work of others. Typically they reports to an Enclave Manager. The RCIO SA/NM/NO is designated as IT-I per AR 25-2.

Minimum Training Requirements

(1). IASO course (https://ia.gordon.army.mil).

(2). IA Technical Level 1 course (SkillPort> CIO G-6/NETCOM Information Assurance> Technical Level I Certification -11 modules) - Approximately 5-7 days

(3). Technical level 2, 10 day SA/NM course. Schedule and locations are located at http://ia.gordon.army.mil. After completion of Tech level II, completion of certification test for Security +, or equivalent draft 8570.1M substitute is required,

Certification Requirements: In order to continue to build to a certified IA workforce for Technical Level III , the SA/NM needs to continue their education and complete one of the certifications in the Technical Level III area. The completion of certification testing is required. The type/s of certification training will be determined by the IA professional's supervisor during the performance evaluation process. The Level III supervisor will notify the IA professional if she/he needs to attend the Level III certification courses held at the NGB or the U.S. Army Reserve (USAR) training facilities. The Security + module in SkillPort build on the Security + certification.

h. Users **to include Foreign Nationals (annual IA training requirement).** The trained and aware employee is the first and most vital line of defense in protecting Information and

Information Systems. This training must be documented by the IASO or IAM. Minimum requirements:

(1) E-learning- US Army Information Assurance Awareness module Approximately 1 Hour.
(2) Users without SkillPort accounts can go to the Fort Gordon website at www.ia.gordon.army.mil to take the User Awareness training- Approximately 1 hour.

(3) MACOM/RCIO/CIO G-6 approved IA awareness training courses.

12. Refresher training: Training for IA positions (IAPM, IANM, IAM, IASO, SA/NM, and DAA, CA) is required every 18-24 months. Either one of the methods will satisfy the refresher training. Methods of training include:

a. Army IA Workshop (held quarterly).
b. E-learning - IA Custom Path Phase II> IDO 470 Security Professional (7 modules)- Approximately 2-3 days (24 hours and 45 minutes).
c. E-learning - IA Custom Path Phase 1> GIAC security fundamentals (15 modules). Approximately 3-5 days.
d. E-learning - IA Technical Level 1 course (11 modules) Approximately 5-7 days.
e. Other service or DoD IA workshops (capture date in A&VTR).

13. Recertification training: Applicable vendor or vendor-neutral recertification (if required to remain certified)

14. Equivalencies/Substitutions

IA workforce personnel in positions of (IAPM, IAM, IASO) are authorized to substitute comparable courses to help individuals prepare for certification exams. Course attendance does not constitute certification. Passing certification exams are mandatory in order for an individual and the Army to meet the draft DoD 8570.1M requirements. The name of the course, course length, course dates, and course sponsor or developer must be identified when tracking completion dates. Equivalent and substitute courses include: CISSP certification, IRMC CIO Certificate program, and NDU Advanced Management Program and other Management and Technical certifications listed in draft DoD 8570.1M.

15. IA tools and training requirements
Users of STAT, Retina, Hercules, and Retina Enterprise Management (REM) will complete the training available at https://iatraining.us.army.mil. Training includes introduction to ISS Monitoring and other online modules on the tools annotated above. Users of ISS Scanner must complete DITYVAP training. Contact ACERT for schedules and availability of training.

16. Tactical Unit IA Awareness training/reporting capability. The IA Workforce should train their users in garrison to minimize bandwidth issues when units are deployed. The tracking of completions will be done through the Army Training Requirements and Resource System (ATRRS) link with SkillPort.

17. References:
AR 25-2, DoDI 8570.1
Draft DoD 8570.1M
Memorandum: Manpower and Reserve Affairs, Payment of Expenses to Obtain Professional Credentials for Army Civilian Employees DTD. 20 June 2003

18. Definitions:

a. Privileged access: Authorized access that provides a capability to alter the properties, behavior, or control of the information system or network. It includes, but is not limited to, any of the following types of access: (a) “Super user,” “root,” or equivalent access, such as access to the control functions of the information system or network, administration of user accounts, and so forth; (b) Access to change control parameters (for example, routing tables, path priorities, addresses) of router, multiplexers, and other key information system or network equipment or software; (c) Ability and authority to control and change program files, and other users’ access to dta; (d) Direct access (also called unmediated access) to functions at the operating-system level that would permit system controls to be bypassed or changed; or (e) Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems or networks (for example, network or system analyzers; intrusion detection software; firewalls) or in performance of cyber or network defense operation.

b. Limited privileged access: Privilege access with limited scope (for example, authority to change user access to data or system resources for a single information system or physically isolated network).

c. Computing Environment: Workstation or server host and its operating system, peripherals, and applications.

d. Network Environment (Computer): The constituent element of an enclave responsible for connecting CE by providing short-haul data transport capabilities, such as local or campus area networks, or long-haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks.

Table 2: IA Workforce Certifications

Certification Provider	**Certification Name**
Computing Technology Industry Association (CompTIA)	A+
CompTIA	Security +
CompTIA	Network+
International Information Systems Security Certifications Consortium ((ISC)2	Certified Information Systems Security Professional (CISSP)
Information Systems Audit and Control Association	Certified Information Security Manager (CISM)
(ISC)2	System Security Certified Practitioner (SSCP)
SecurityCertified.Net	Security Certified Network Professional (SCNP)
SecurityCertified.Net	Security Certified Network Architect (SCNA)
SANS Institute	GIAC Security Essentials Certification (GSEC)
SANS Institute	GIAC Security Leadership Certificate (GSLC)
SANS Institute	GIAC Security Expert (GSE)
SANS Institute	GIAC Information Security Fundamentals (GISF)
CyberTrust	TruSecure ICSA Certified Security Associate (TICSA)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Auditor
